**(The answer is in the end)**

**PAHS Financial Literacy / Identity theft and phishing scams**

Lesson Objectives: Students will be able to:

• List the common techniques used to steal one’s identity.

• Become aware of electronic phishing ploys.

• Describe and evaluate methods to protect financial records.

• Explain how to take action if your identity is stolen.

• Explain behavior to operate more safely online and with mobile devices.

“Today we are going to learn about a fast-growing financial crime: identity theft. You will be able to list the common techniques used to steal one’s identity and know how to report that one’s identity is stolen. You will be able to list some behaviors to protect your financial records and personal information and to operate more safely online and with mobile devices.”

The Lesson Procedure:

If you have ever heard a parent or a relative say when they opened their credit card bill, “Wow, I did not charge all of these things. I did not buy that $500 watch!”, it is possible that they were a victim of identity theft. FTC surveys show that about 10 million people are victims of identity theft each year. People who are dishonest and unethical (and they are often very smart) will try to make their money by stealing yours. Identity theft is a crime.

***Definitions:***

Identity theft is when a person acquires and then uses your name (and address, Social Security Number) in order to apply for a credit card in your name or purchase products in your name.

Phishing occurs with electronic communication such as e-mail or text messaging. It is when someone pretends to be someone or something they are not to acquire your passwords, credit card or bank account information, or other personal information.

FTC: The Federal Trade Commission an independent federal government agency (since 1914) whose mission is to promote consumer protection and help deter anti-competitive and unethical business practices such as deceptive advertising, phishing, and identity theft.

Watch instructional videos by the Federal Trade Commission on identity theft.

* “Identity Theft” (1 minute, 8 seconds) at: <http://www.youtube.com/watch?v=-IEBVIh7bzc>
* CBS News item (4 min) <https://www.youtube.com/watch?v=DT9DoS-1QgQ>
* FTC – Identity Theft.mp4 (1 minute, 53 seconds) at: <http://www.youtube.com/watch?v=OoPJImjP1ZQ>
* Watch a video on phishing, “Phishing Scams in Plain English” (3 minutes, 5 seconds) at: <http://www.youtube.com/watch?v=sqRZGhiHGxg&feature=relmfu>

Review the major points of the videos.

The top methods for stealing a person’s identity are:

1. “Dumpster Diving”: going through a person’s or household’s trash to look for credit card offers, bills, bank account numbers, pay stubs, anything with Social Security numbers, birth dates, bank or credit account number, or other personal information.

2. Skimming: stealing credit card numbers with a small hand-held unit that can store your credit card number with a quick swipe of your card.

3. Phishing: pretending to be a legitimate financial institution, government agency, or company though an e-mail, a pop-up message, a text message, etc.

4. Changing your address: Completing a change of address card at the Post Office to defer your mail to another location other than your home. Or hacking into your e-mail or online accounts to change your address or steal your personal information.

5. Stealing: stealing mail from a person’s U.S. postal service mailbox, or stealing your mailed Income Tax Return; stealing wallets or purses; bribing employees who have access to employee personnel records.

Can think of other, unscrupulous methods for attempting to steal one’s identity or cleverly disguise phishing? Have you ever received a spam text message?

Write a list of the harmful things that could occur if your identity is stolen, for example:

• Someone could withdraw money from your bank account using a debit card or credit card in your name.

• Your credit score could drop if you exceed your credit limit.

• You have to take the time and go through the expense of cancelling accounts, getting new accounts and account numbers, etc.

What to do if you are a victim of Identity Theft

The FTC’s website is a one-stop resource to both learn about identity theft and walk you through the appropriate actions if your identity is stolen: <http://www.ftc.gov/bcp/edu/microsites/idtheft/>

Some steps include:

• Report the identity theft to the 3 credit bureaus: Experian, TransUnion, and Equifax.

• File a police report with local law enforcement.

• Report the theft to the FTC online at [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft) or by phoning 1-877-ID-THEFT (1-877-438-4338).

Deterring Identity Theft:

Create a list of behaviors to deter thieves from stealing your identity, such as:

• Shred financial documents that are not being kept for safeguarding. [This allows a teacher to cover the kind of information that should be held and for how long (in years). It also allows a teacher to cover what documents are best kept in a safe deposit box, a home safe, regular home files, etc.]

• Do not carry around your Social Security Card in your wallet.

• Do not give out personal information over the phone or over the internet unless you are absolutely sure who you are dealing with.

• Choose computer and electronic passwords with care by avoiding birth dates, your Social Security Number, your mother’s last name, etc.

• Try not to have your postal mail pile up in your mailbox for several days; if you are going to be away for a few days, have your mail held at the post office until you return.

• Do not click on suspicious links in e-mail or complete forms with your account number and password. Check the web address.

• Be suspicious about regular bills that do not arrive on time, denials of credit for no apparent reason, calls or letters about purchases you did not make, charges on your financial statements that you do not recognize.

• Use a password to access your mobile devices such as your cell phone, tablet (iPad), etc., just as you would have a password to get access to your e-mail accounts.

Closing the Lesson:

**Describe why it is important to protect one’s financial documents/identity.**

Because that’s who you are.

**What can you do to protect your identity from being stolen?**

Take steps to protect yourself from identity theft:

* Secure your social security number (SSN). Don’t carry your social security card in your wallet or write your number on your checks. Only give out your SSN when absolutely necessary.
* Don’t respond to unsolicited requests for personal information (your name, birthdate, social security number, or bank account number) by phone, mail, or online.
* Watch out for “shoulder surfers.” Shield the keypad when typing your passwords on computers and at ATMs.
* Collect mail promptly. Ask the post office to put your mail on hold when you are away from home for several days.
* Pay attention to your billing cycles. If bills or financial statements are late, contact the sender.
* Review your receipts. Promptly compare receipts with account statements. Watch for unauthorized transactions.
* Shred receipts, credit offers, account statements, and expired cards, to prevent “dumpster divers” from getting your personal information.
* Store personal information in a safe place at home and at work.
* Install firewalls and virus-detection software on your home computer.
* [Create complex passwords](https://www.consumer.ftc.gov/blog/advanced-password-tips-and-tricks) that identity thieves cannot guess easily. Change your passwords if a company that you do business with has a breach of its databases
* [Order your credit report](http://www.annualcreditreport.com/) once a year and review to be certain that it doesn't include accounts that you have not opened. Check it more frequently if you suspect someone has gained access to your account information.

**What steps should you take if your identity is stolen?**

• Report the identity theft to the 3 credit bureaus: Experian, TransUnion, and Equifax.

• File a police report with local law enforcement.

• Report the theft to the FTC online at [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft) or by phoning 1-877-ID-THEFT (1-877-438-4338).

**What kinds of tactics are used online with phishing scams?**

Phishing: pretending to be a legitimate financial institution, government agency, or company though an e-mail, a pop-up message, a text message, etc.